Confidentiality, Privacy and Security (CPS) Workgroup Testimony

by
William R. "Bill" Braithwaite, MD, PhD, FACMI

June 22, 2007

HIPAA Privacy and Security Rules for eHIE

Although drafts as early as 1993 of the language that would eventually become part of HIPAA included text about "…standards, conventions, and requirements related to the inclusion of data from patient care records into the health care data interchange system …", the Administrative Simplification Subtitle of the Health Insurance Portability and Accountability Act (HIPAA) as passed in 1996 was written only to apply federal standards to the specific use case of electronic financial and administrative transactions. As such, the applicability of the law and the subsequent regulations was limited to covered entities, defined as "a health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a transaction referred to in [the section on Standards to Enable Electronic Exchange]."

Also removed from early drafts was specific language for privacy standards. What remained was a requirement for the Secretary of HHS to submit "… detailed recommendations on standards with respect to the privacy of individually identifiable health information ..." and a backup position to an implied promise that Congress would pass a comprehensive health information privacy law within three years.

> "If legislation governing standards with respect to the privacy of individually identifiable health information transmitted in connection with the transactions … is not enacted by the date that is 36 months after the date of the enactment of this Act, the Secretary of Health and Human Services shall promulgate final regulations containing such standards not later than the date that is 42 months after the date of the enactment of this Act."

Despite the lack of specific legislative direction, HHS promulgated a comprehensive set of regulations covering the privacy and security of health information based on a well exercised set of principles[1] that had been used for over 2 decades as the basis for privacy law in other instances and other countries. Those are:

Notice

The existence and purpose of record-keeping systems must be known to the individuals whose data is contained therein.

Choice

Information must be collected only with the knowledge and implicit or explicit permission of the subject, used only in ways relevant to the purpose for which the data was collected, and disclosed

[1] First described in "Records, Computers and the Rights of Citizens." Report of the Secretary's Advisory Committee on Automated Personal Data Systems. July, 1973. (See http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm)

only with permission of the subject or in accordance with overriding legal authority (such as a public health law that requires reporting of a serious contagious disease).

Access

Individuals must have the right to see records of information about them and to assure the quality of that information (accuracy, completeness, and timeliness). In healthcare, records are rarely deleted or replaced, but this principle implies that there is at least a due process for individuals to amend poor quality information about them.

Security

Reasonable safeguards must be in place for the confidentiality, integrity, and availability of information.

Enforcement

Violations must result in reasonable and consistently applied penalties to deter violators and in reasonable mitigation efforts to offset the effects of a breach as much as possible.

Because it didn't make much sense to have privacy and security regulations only apply to covered entities, HHS came up with the concept of business associates to extend the protections afforded by the rules under contracts to those to whom covered entities were outsourcing work on patients' information. Despite a slow start, I believe the covered entities of the health care industry have adapted well to the HIPAA Privacy and Security Rule requirements.

However, many things about healthcare have changed since the publication of the Privacy Rule in December 2000. Because of the limited applicability of the HIPAA law and its subsequent regulations, there is uncertainty about the status of recently developed regional health information exchange organizations and personal health record sponsors. They are not health care providers, health plans, or health care clearinghouses under the HIPAA definitions and may or may not be business associates of these covered entities. They did not exist and therefore were not considered when the law and the regulations were being written.

Last year, HHS contracted with RTI and subcontractors in 33 states and Puerto Rico to perform assessments of organization-level privacy- and security-related policies, practices, laws, and regulations that affect interoperable health information exchange and to propose privacy and security protections that permit interoperability. That project, the Health Information Security and Privacy Collaboration (HISPC), is in the process of finishing the final report on its findings. The project found many variations in practice that were perceived to be barriers to eHIE and many of these results reveal the difficulty of applying HIPAA to this forthcoming electronic health information exchange environment.

Sources of Variation in Privacy and Security Practices

HISPC found four main sources of variations in business practices which could be barriers to eHIE:

1) Variation related to misunderstandings and differing applications of federal laws and regulations including:

a) the HIPAA Privacy Rule, particularly issues of patient authorization/consent and the determination of "Minimum Necessary".
b) the HIPAA Security Rule, particularly confusion regarding the different types of security required and misunderstandings regarding what is currently technically available and scalable.
c) 42 CFR part 2, particularly lack of understanding by treatment facilities, physicians, and integrated delivery systems about 42 CFR part 2, its relation to HIPAA, and the application of each regulation.

2) Variation related to state privacy laws, which were found scattered throughout many chapters of law and, when found, were often conflicting and antiquated because they were written for a paper-based system.
3) Lack of trust in applied information security, both by one organization toward others and by consumers/patients toward organizations other than their own healthcare providers.
4) Cultural and business issues, including concern about liability for incidental or inappropriate disclosures and general resistance to change.

From my personal perspective as one of the advisors on this project, these variations are due in most part to fear, uncertainty, and doubt. Decision-makers fear violating state or federal laws that are not well understood, and therefore they are fearful of making 'reasonable' decisions as directed by the HIPAA rules. Their fear of liability (personal and financial) leads to them taking a very conservative approach, which tends to impede the sharing of health information outside their own institution.

Uncertainty exists across the range of patients and healthcare employees (including some lawyers) about the rights and responsibilities under the complex set of federal and state laws and regulations. Organizations are uncertain as to exactly how to interpret HIPAA's "reasonable safeguards" guidelines consistently. Enforcement actions may be 'reasonable' from the government's perspective but some implementers want to know how the rules are being interpreted by the enforcers so they can be comfortable with their own decisions. There is no standard set of technology to implement eHIE; variations in communications media create difficulties in information exchange and non-uniform implementation of encryption and other security technology impair electronic methods of health information exchange.

There is doubt about the value of investing in technologies for information safeguards by small, financially strapped organizations and a lingering doubt about ROI and/or its timing among larger, high-tech organizations.

The state teams under this project have proposed several state-level solutions to these barriers:

1) Governance — Most call for a permanent body to oversee and guide implementation of privacy and security solutions.
2) Business practices and policies solutions — Most call for standardization (using model forms, contracts, policies, and processes) of business practices for consent and authorization, application of federal law, exchange of sensitive information, and exchange of data related to Medicaid, public health, and law enforcement agencies.
3) Legal and regulatory solutions — Most call for amending state law and introducing new legislation where required.

4) Technological solutions — Most call for standardized approaches to patient identification systems; authorization, authentication, access, and audit; segmenting data within electronic medical records; terminology standards; and transmission security standards.
5) Education and outreach — All call for both consumer and provider education and outreach.

In a recent report[2], the GAO identified key challenges associated with protecting electronic personal health information in four areas:

1) Understanding and resolving legal and policy issues:
   a) Resolving uncertainties regarding the extent of federal privacy protection required of various organizations
   b) Understanding and resolving data sharing issues introduced by varying state privacy laws and organization-level practices
   c) Reaching agreements on differing interpretations and applications of the HIPAA privacy and security rules
   d) Determining liability and enforcing sanctions in case of breaches of confidentiality
2) Ensuring appropriate disclosure:
   a) Determining the minimum data necessary that can be disclosed in order for requesters to accomplish their intended purposes
   b) Determining the best way to allow patients to participate in and consent to electronic health information exchange
   c) Educating consumers about the extent to which their consent to use and disclose health information applies
3) Ensuring individuals' rights to request access and amendments to health information:
   a) Ensuring that individuals understand that they have rights to request access and amendments to their own health information
   b) Ensuring that individuals' amendments are properly made and tracked across multiple locations
4) Implementing adequate security measures for protecting health information:
   a) Determining and implementing adequate techniques for authenticating requesters of health information
   b) Implementing proper access controls and maintaining adequate audit trails for monitoring access to health data
   c) Protecting data stored on portable devices and transmitted between business partners

These challenges are compatible with the results of the HISPC project and I expect its final report will discuss solutions to resolve many of them. The GAO report also recommends that HHS "Ensure that key privacy principles in HIPAA are fully addressed."

Everyone seems to agree that, as much as possible, there should be a "level playing field" (i.e., everyone follows the same rules) for participating in an electronic health information exchange network, regardless of the participants' "status" under the HIPAA Privacy and Security Rules. However, it is also clear that if everyone was suddenly subject to the rules as covered entities, it would not be enough to resolve the issues or meet the challenges above.

---

[2] GAO-07-988T, a testimony before the House Subcommittee on Information Policy, Census, and National Archives; Committee on Oversight and Government Reform. (See www.gao.gov/cgi-bin/getrpt?GAO-07-988T)

There are several different alternative approaches to consider, but not all may be practical.

1) **New Comprehensive Federal Law.** – Federal law has the advantage of being able to cover all participants equally but has several significant disadvantages as well. The most obvious is the difficulty of getting a law passed[3]. Another is the difficulty of balancing state's rights in this area with the need for the level playing field. There are significant cultural differences in attitudes about privacy and consent between states and people feel very strongly about their positions on these issues. There are also several different types of new federal law that could be passed to address these issues:
   a) **Non-discrimination law**. – If it were made illegal for organizations to discriminate against individuals based on their health status, the major motivation for people to keep their health information secret would disappear and the residual issues that truly related to privacy could be dealt with more easily.
   b) **Comprehensive privacy law**. – If we took the approach used by the EU[4] and passed a law that requires each of the states to pass laws that meet certain criteria based on the principles of fair information practice, we could give the states the flexibility they want but could set the criteria to level the playing field for eHIE. The downside would be that states that signed up for such an approach could not sent individually identifiable data to states that had not signed up without special negotiations that may be a bad as what we have now.
   c) **Comprehensive health information privacy law**. – If we could pass a law like the one that was promised by HIPAA, we could set the applicability to any person who handles the individually identifiable health information of another person and limit state variability to enable eHIE. This would allow the protections of HIPAA privacy and security rules to follow the information, wherever it goes, rather than only covering specifically named entities.
2) **Federal law modifying HIPAA**. – Instead of trying to pass a new, comprehensive federal law, it might be more feasible to pass a law that adds the new types of organizations that handle individually identifiable health information, such as PHR vendors and eHIE organizations, to the definition of covered entity in HIPAA. Including requirements in the law for standards for specific clinical information transactions could justify these additions. eHIE organizations could then be classified as health care clearinghouses and PHR vendors would have to be added as covered entities because of their direct interactions with patients. Without such a modification to the HIPAA law, these changes could not be made through regulation alone because the current HIPAA language excludes them.
3) **Model Law for states**. – If the states could agree to pass laws based on a common model that builds upon HIPAA, similar to the successful passage and use of the Uniform

[3] In contrast to other industrialized countries throughout the world, the U.S. has not codified the Fair Information Principles into an omnibus privacy law at the federal level, despite several attempts. Instead, many individual laws have been passed, at both federal and state levels, addressing specific business sectors or practices. Examples are the Fair Credit Reporting Act, the Right to Financial Privacy Act, the Electronic Communications Privacy Act, and the Video Privacy Protection Act. The U.S. does have the Privacy Act of 1974, but this statute only protects personal information held by federal government agencies.

[4] The European Union's Directive on Protection of Personal Data was approved in June 1995 to establish a stable regulatory framework to enable the movement of personal data from one country to another, while at the same time ensuring that privacy protection is "adequate" in the country to which the data is sent. If the recipient country has not established a minimum standard of data protection, it is expected that the transfer of data will be prohibited.

Commercial Code (UCC), we could level the playing field while allowing some controlled and understood variability across states.

My conclusion is that the HIPAA privacy and security rules have a sound basis, but their implementation has been protracted. Much work is currently underway to resolve some of the challenges to implementing HIPAA privacy and security rules appropriately. However, the healthcare industry is changing quickly and HIPAA cannot adequately cover new situations and entities that were not considered in the original law, including independent PHR service providers and eHIE organizations. Whatever alternative solutions are chosen, the principled approach to privacy and security taken under HIPAA can serve as a guide in applying the principles of fair information practice to such new environments.